

CLAIMS

What is claimed is:

- 1 1. A multi-function peripheral device comprising:
2 a virus protection process configured to
3 detect that one or more unauthorized instructions have been stored on the
4 multi-function peripheral; and
5 in response to detecting that one or more unauthorized instructions have been
6 stored on the multi-function peripheral, perform one or more actions to
7 address the one or more unauthorized instructions that have been
8 stored on the multi-function peripheral.

- 1 2. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is configured to detect that one or more unauthorized instructions
3 have been stored on the multi-function peripheral by periodically examining,
4 according to specified configuration criteria, data stored on the multi-function
5 peripheral to determine whether the data has been modified in an unauthorized
6 manner.

- 1 3. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is configured to detect that one or more unauthorized instructions
3 have been stored on the multi-function peripheral by examining and detecting that one
4 or more data files stored on the multi-function peripheral have been modified.

1 4. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is configured to detect that one or more unauthorized instructions
3 have been stored on the multi-function peripheral by examining and detecting that
4 program code stored on the multi-function peripheral has been modified.

1 5. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is configured to detect that one or more unauthorized instructions
3 have been stored on the multi-function peripheral by examining and detecting that
4 configuration data stored on the multi-function peripheral has been modified.

1 6. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is configured to examine data stored on a non-volatile memory of
3 the multi-function peripheral.

1 7. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is configured to examine data stored in a volatile memory of the
3 multi-function peripheral.

1 8. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is further configured to undo changes made as a result of execution
3 of the one or more unauthorized instructions.

1 9. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is further configured to
3 determine whether particular data stored on the multi-function peripheral can
4 be restored to a prior state; and
5 in response to determining that the particular data cannot be restored to the
6 prior state, then delete the particular data from the multi-function
7 peripheral.

1 10. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is further configured to render the one or more instructions
3 inaccessible and unexecutable on the multi-function peripheral.

1 11. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is further configured to notify a user via a graphical user interface
3 on the multi-function peripheral that the storage of the one or more unauthorized
4 instructions on the multi-function peripheral has been detected.

1 12. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is further configured to notify a user by printing a report on the
3 multi-function peripheral that indicates that the storage of the one or more
4 unauthorized instructions on the multi-function peripheral has been detected.

1 13. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is further configured to provide notification via an email that the
3 storage of the one or more unauthorized instructions on the multi-function peripheral
4 has been detected.

1 14. The multi-function peripheral device as recited in Claim 1, wherein the virus
2 protection process is further configured to provide notification via a facsimile that the
3 storage of the one or more unauthorized instructions on the multi-function peripheral
4 has been detected.

1 15. The multi-function peripheral device as recited in Claim 1, wherein the multi-function
2 peripheral is configured to receive, over a network, data used by the virus protection
3 process to detect that the one or more unauthorized instructions have been stored on
4 the multi-function peripheral.